Formation Mettre en oeuvre et configurer la solution Cisco Identity Services Engine

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour déployer et utiliser Cisco Identity Services Engine (ISE) v3.x, une plateforme de politique d'identité et de contrôle d'accès qui simplifie la fourniture d'un contrôle d'accès cohérent et hautement sécurisé à travers des connexions câblées, sans fil et VPN. Les participants apprendront à mettre en oeuvre et appliquer les fonctionnalités de Cisco ISE afin de prendre en charge les cas d'utilisation de la posture de sécurité Zero Trust. Ces cas d'utilisation incluent des tâches telles que l'application des politiques, les services de profilage, l'authentification Web et les services d'accès des invités, le BYOD, les services de conformité des terminaux et l'administration des périphériques TACACS+. La formation apprend également à déployer et à utiliser Cisco® Identity Services Engine (ISE) v3.x, une plateforme de politique d'identité et de contrôle d'accès qui simplifie la fourniture d'un contrôle d'accès cohérent et hautement sécurisé à travers des connexions câblées, sans fil et VPN. Cette formation vous permet également d'obtenir 40 crédits de formation continue (CE) en vue d'une recertification.

Référence	SISE
Durée	5 jours (35h)
Tarif	4 190 €HT
Repas	100 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 2 au 6 juin 2025
du 8 au 12 septembre 2025
du 22 au 26 septembre 2025
du 29 sept. au 3 octobre 2025
du 17 au 21 novembre 2025

PARIS

du 8 au 12 septembre 2025
du 22 au 26 septembre 2025
du 29 sept. au 3 octobre 2025
du 17 au 21 novembre 2025
du 9 au 13 février 2026

VOIR TOUTES LES DATES

Objectifs

| Expliquer le déploiement de Cisco ISE
| Décrire les composants d'application de la politique de Cisco ISE
| Décrire la configuration de la politique de Cisco ISE
| Dépanner la politique de Cisco ISE et la prise en charge des dispositifs d'accès au réseau (NAD) par des tiers
| Configurer l'accès des invités et les hotspots et les portails invités
| Décrire les services de profilage de Cisco ISE
| Décrire les meilleures pratiques de profilage et les rapports
| Configurer une solution Cisco ISE BYOD, la conformité des points d'extrémité et les services de posture client
| Configurer l'administration des appareils Cisco ISE
| Décrire les configurations de Cisco ISE TrustSec

Public

| personnes impliquées dans le déploiement et la maintenance d'une solution Cisco Identity Services Engine.

Prérequis

| Familiarité avec l'interface de ligne de commande (CLI) du logiciel Cisco IOS® pour les périphériques câblés et sans fil
| Familiarité avec Cisco AnyConnect® Secure Mobility Client
| Familiarité avec les systèmes d'exploitation Microsoft Windows
| Connaissance de la norme 802.1x

Programme de la formation

Présentation de l'architecture de Cisco ISE
| Cisco ISE en tant que moteur de politique d'accès au réseau
| Cas d'utilisation de l'ISE de Cisco

| Fonctions de l'ISE de Cisco

Introduction au déploiement de Cisco ISE
| Modèles de déploiement de Cisco ISE
| Exigences de licence et de réseau de Cisco ISE
| Fonctionnalités de visibilité du contexte de Cisco ISE
| Nouvelles fonctionnalités de Cisco ISE 3.X
| Configuration initiale de Cisco ISE et utilisation des certificats système

Présentation des composants d'application des politiques de Cisco ISE
| 802.1X pour l'accès câblé et sans fil
| Contournement de l'authentification MAC pour l'accès câblé et sans fil
| Gestion de l'identité
| Source d'identité Active Directory
| Autres sources d'identité
| Services de certificats
| Intégrer Cisco ISE à Active Directory

Introduction à la configuration des politiques de Cisco ISE
| Politique de Cisco ISE
| Règles d'authentification Cisco ISE
| Règles d'autorisation de Cisco ISE
| Configurer la politique Cisco ISE pour MAB
| Configurer la politique Cisco ISE pour 802.1X

Dépannage de la politique Cisco ISE et du support NAD tiers
| Prise en charge des périphériques d'accès au réseau tiers de Cisco ISE
| Dépannage de la configuration de la politique de Cisco ISE

Présentation de l'authentification Web et des services aux invités
| Accès Web avec Cisco ISE
| Composants de l'accès invité
| Paramètres d'accès des visiteurs
| Configurer l'accès invité

Configuration des Hotspots et des portails d'invités
| Configuration des portails sponsors et invités
| Configurer le Hotspot et l'accès des invités auto-enregistrés
| Configurer l'accès des invités approuvés par le sponsor et entièrement sponsorisés
| Créer des rapports sur les invités

Présentation du profileur Cisco ISE
| Présentation du profileur ISE
| Sondes Cisco ISE
| Politique de profilage
| Configurer le profilage
| Personnaliser la configuration du profileur Cisco ISE

Présentation des meilleures pratiques et des rapports de profilage
| Meilleures pratiques de profilage
| Créer des rapports de profilage Cisco ISE

Configurer Cisco ISE BYOD
| Présentation de la solution Cisco ISE BYOD
| Flux Cisco ISE BYOD
| Configuration du portail My Devices
| Configuration des certificats dans les scénarios BYOD
| Configurer BYOD
| Gérer un appareil BYOD perdu ou volé

Présentation de Cisco ISE Endpoint Compliance Services
| Présentation des services de conformité des points finaux
| Configurer les services de conformité Cisco ISE

Configurer les services de posture du client et la conformité
| Configuration des services de protection du client et de l'approvisionnement
| Configurer l'approvisionnement du client
| Configuration des politiques de sécurité
| Test et surveillance de l'accès basé sur la conformité

Travailler avec des dispositifs d'accès au réseau
| Révision de AAA
| Administration des périphériques TACACS+ de Cisco ISE
| Configuration de l'administration des dispositifs TACACS
| Lignes directrices et meilleures pratiques pour l'administration des dispositifs TACACS+
| Migration de Cisco ACS vers Cisco ISE
| Configurer Cisco ISE pour l'administration de base des équipements
| Configurer l'autorisation de commande de Cisco ISE

Explorer Cisco TrustSec
| Présentation de Cisco TrustSec
| Améliorations de Cisco TrustSec
| Configuration de Cisco TrustSec
| Configurer Cisco TrustSec

Labs :
| Lab 1A : Installation et configuration de base de Cisco ISE
| Lab 1B : Vérifier la configuration initiale de Cisco ISE et l'utilisation des certificats système
| Lab 2 : Intégrer Cisco ISE avec Active Directory
| Lab 3 : Configurer la politique de Cisco ISE pour MAB
| Lab 4 : Configurer la politique Cisco ISE pour 802.1X
| Lab 5 : Configurer l'accès invité
| Lab 6 : Configurer le Hotspot et l'accès invité auto-enregistré
| Lab 7 : Configurer l'accès des invités approuvés par les sponsors et entièrement sponsorisés
| Lab 8 : Créer des rapports sur les invités
| Lab 9 : Configurer le profilage
| Lab 10 : Personnaliser la configuration du profilage de Cisco ISE
| Lab 11 : Créer des rapports de profilage Cisco ISE
| Lab 12 : Configurer le BYOD
| Lab 13 : Gérer un appareil BYOD perdu ou volé
| Lab 14 : Configurer les services de conformité de Cisco ISE
| Lab 15 : Configurer l'approvisionnement des clients
| Lab 16 : Configurer les politiques de posture
| Lab 17 : Tester et surveiller l'accès basé sur la conformité
| Lab 18 : Configurer Cisco ISE pour l'administration de base des appareils
| Lab 19 : Configurer l'autorisation de commande Cisco ISE
| Lab 20 : Configurer Cisco TrustSec

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.